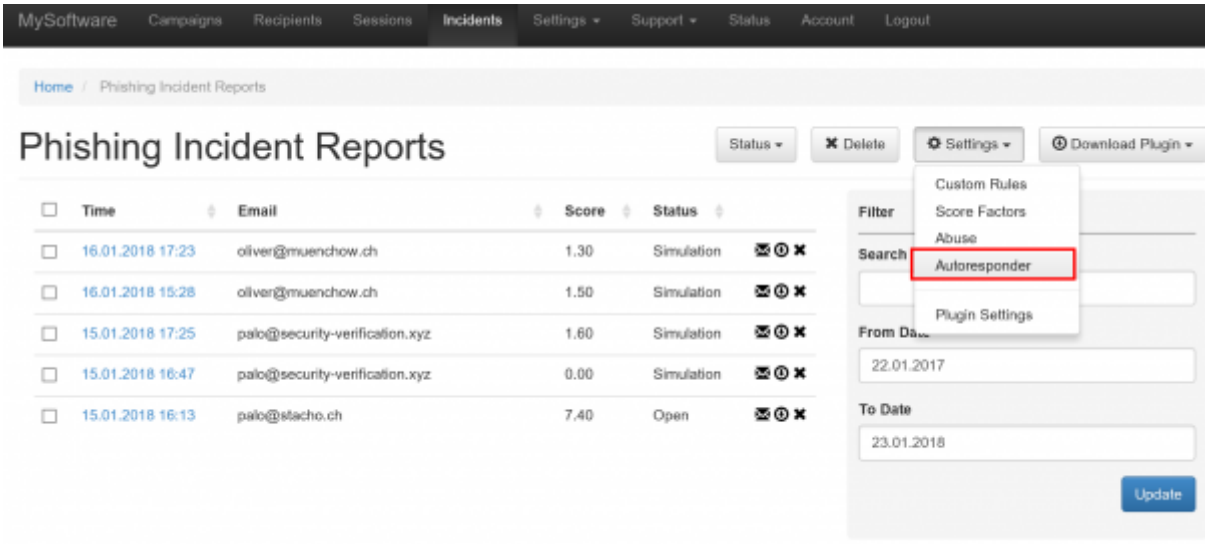
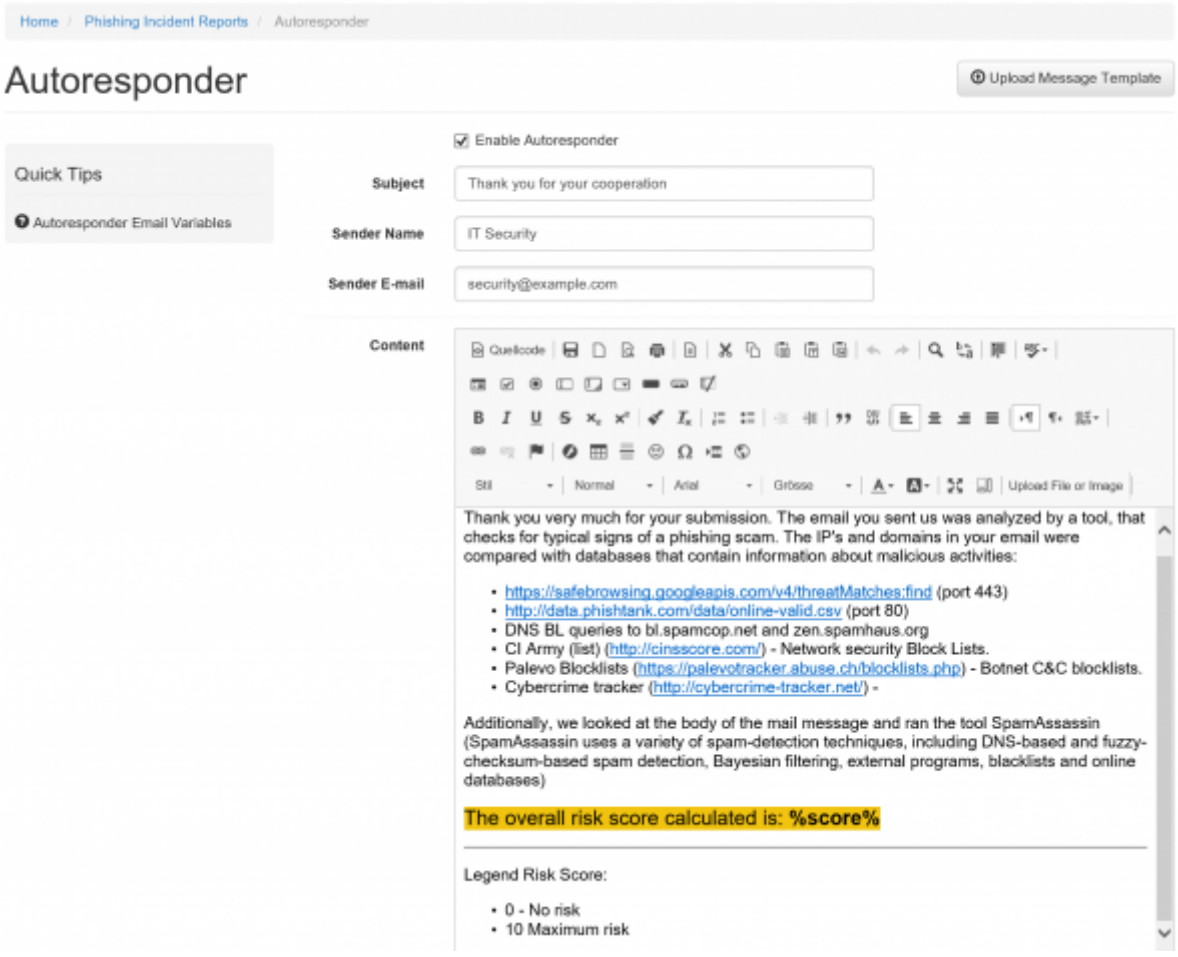
Incident Auto Responder

LUCY allows the admin to define an auto responder for submitted emails through the phish button.



The message may contain the actual risk score calculated in LUCY.



The risk score uses the IP's and domains in your email and compares them with databases that contain information about malicious activities:

- https://safebrowsing.googleapis.com/v4/threatMatches:find (port 443)
- http://data.phishtank.com/data/online-valid.csv (port 80)
- DNS BL queries to bl.spamcop.net and zen.spamhaus.org
- CI Army (list) (http://cinsscore.com/) - Network security Block Lists.
- Palevo Blocklists (https://palevotracker.abuse.ch/blocklists.php) - Botnet C&C blocklists.
- Cybercrime tracker (http://cybercrime-tracker.net/) -

Additionally, we look at the body of the mail message and run the tool SpamAssassin (SpamAssassin uses a variety of spam-detection techniques, including DNS-based and fuzzy-checksum-based spam detection, Bayesian filtering, external programs, blacklists and online databases).

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=incident_auto_responder&rev=1516628222

Last update: **2019/07/25 12:51**